REMARKS

I. General

Claims 1-17 were pending in the present application, and all of such claims were rejected in a Final Office Action mailed September 15, 2005. In response to the Final Office Action, Applicant filed a notice of appeal and a supporting appeal brief traversing the rejections raised in the Final Office Action. In response to the appeal brief, the Examiner did not file an Answer, but instead responded with the current Office Action (mailed April 7, 2006) which reopens prosecution and raises new grounds of rejection. The outstanding issues raised in the current Office Action are:

- Claims 1-2, 8, 13-14, and 16 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,728,885 to Taylor et al. (hereinafter "*Taylor*"); and

- Claims 3-7, 9-12, 15, and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Taylor* in view of U.S. Patent No. 5,987,611 to Freund (hereinafter "*Freund*").

In response, Applicant respectfully traverses the outstanding claim rejections, and requests reconsideration and withdrawal thereof in light of the amendments and remarks presented herein.

II. Amendments

Claims 1-2 and 13 are amended, and new claims 18-20 are added herein. No new matter is presented by these claim amendments and additions.

More specifically, claim 1 is amended to recite "the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule" (newly added language shown underlined). This amendment further clarifies the recited at least one field of the text-file. Support for this amendment can be found, *inter alia*, at page 17, line 8 – page 21, line 2 of the specification of the present application.

Claim 2 is amended to recite that the "at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field" (newly added language shown underlined).

Claim 13 is amended to replace "the network-exploit rule" with "a network-exploit rule" to resolve a potential antecedent basis issue for this term. This amendment is not intended to narrow the scope of claim 13 in any way, but is rather intended solely as a cosmetic amendment to ensure that the term "network-exploit rule" is properly introduced in the claim.

New claims 18-20 are added, and support for such claims can be found, *inter alia*, at page 17, line 8 – page 21, line 2 of the specification of the present application.

III. Rejections Under 35 U.S.C. § 102 over *Taylor*

Claims 1-2, 8, 13-14, and 16 are rejected under 35 U.S.C. § 102(e) as being anticipated by *Taylor*. Applicant respectfully traverses this rejection as provided further below.

To anticipate a claim under 35 U.S.C. § 102, a single reference must teach every element of the claim, *see* M.P.E.P. § 2131. Applicant respectfully submits that *Taylor* fails to teach each and every element of claims 1-2, 8, 13-14, and 16, as discussed further below.

Independent Claim 1

Claim 1, as amended herein, recites in part "an operating system ... operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule" (emphasis added). *Taylor* fails to teach at least the above-emphasized element of claim 1.

That is, *Taylor* does not teach a text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system (IPS) evaluates the network-exploit rule. Rather, *Taylor* appears to describe a configuration file that specifies to a firewall rules regarding whether a connection is permitted on particular ports, as well as rules regarding filtering packets for a permitted connection. *See* Col. 5, line 66 – Col. 6, line 60 of *Taylor*. While actions (e.g., filtering packets) for a given rule are only taken by the firewall if the corresponding rule is satisfied, the rules specified in the configuration file appear to all be evaluated by the firewall. *Taylor* does not teach that the configuration file comprises at least one field that includes information from which a determination is made as to whether an IPS evaluates the network-exploit rule. No determination of whether an intrusion protection system is to evaluate a rule is made in *Taylor*, but instead *Taylor* appears to teach that all rules defined in its configuration file are all evaluated irrespective of any information contained in the configuration file. Again, when evaluated, a determination may be made that a rule is not satisfied under certain circumstances, and thus the corresponding actions (e.g., filtering packets) may not be applied; but in all cases of *Taylor* all rules defined in the configuration file appear to be evaluated.

Thus, *Taylor* does not provide any teaching whatsoever of including at least one field in its configuration file from which a determination is made as to whether a network-exploit rule in the configuration file is to be evaluated by an IPS, which potentially leads to inefficient processing if rules are defined in the configuration file that are not desired to be evaluated, *see e.g.,* page 17, line 8 – page 21, line 2 of the specification of the present application.

In view of the above, *Taylor* fails to teach all elements of claim 1, and therefore claim 1 is not anticipated by *Taylor*. Therefore, the rejection of claim 1 should be withdrawn.

Independent Claim 8

Claim 8 recites in part "specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file." *Taylor* fails to teach at least this element of claim 8.

Taylor does not teach specifying an ENABLED field value or a SEVERITY level field value during generation of a text file. Rather, *Taylor* appears to describe a configuration file that specifies to a firewall rules regarding whether a connection is permitted on particular ports, as well as rules regarding filtering packets for a permitted connection. *See* Col. 5, line 66 – Col. 6, line 60 of *Taylor*. *Taylor* provides no teaching whatsoever of specifying an ENABLED field value or a SEVERITY level field value during generation of its configuration file. *Taylor* provides no teaching of such fields in its configuration file.

In rejecting claim 8, the current Office Action relies upon its reasoning presented for claim 2, which cites to Col. 6, lines 31-57 and Col. 10, line 51 – Col. 11, line 32 of *Taylor* as teaching this element, *see* pages 3-4 of the Office Action. The cited portions of *Taylor* are as follows:

> Another dynamic filter rule is a selective filtering rule. This rule requires proxy 211 to handle connection control packets and packet filters to handle the data packets. In other words, the packet filtering will be enabled only when proxy 211 has performed it's security checks for the connections, i.e., checking the relevant information on the SYN packet sent by DPF 207. For instance, this rule is useful for protocols such as File Transfer Protocol (FTP), which sends data packets on a different connection after establishing the connection. Other filtering rules are also possible such as not applying any filtering or applying a proxy filter at the application layer to all packets received on a specific connection.
>
> The configuration file discussed above, which stored the information on which ports are registered, further includes various filter rules to be applied for specific connections. For example, packets received from a particular port can be subjected to the filter all rule filter, while packets received from another port can be subjected to the selective filtering rule. The configuration file is preferably stored in the computer where firewall 201 is located. It should be noted, however, that the configuration file can be stored in any of internal hosts. It should also be noted that the system administrator creates the configuration information file discussed above and specifies the TPF rules by utilizing a graphical user interface configured receive appropriate information from the system administrator. (Col. 6, lines 31-57).
>
> It should be noted that the above described program functions and associated data structure formats are implemented in computer programs such as C or C++. Alternatively, the computer programs can be written in other computer languages such as Pascal.

> Referring back to FIG. 4, in order to continue on with the description of steps that take place during operation of firewall 201, in step 321, DPF 207 determines whether the packet matches with any of user specified rules. (This steps is performed when the port on which the communication establishing packet was received is not registered.) Whether the packet matches a user specified rule is determined by attribute information of the packet. The attribute information of the packet includes:
>
> Source and destination computer addresses;
>
> Source and destination transport layer protocol numbers;
>
> Type of protocol (TCP, UDP etc.); and
>
> Port numbers of NIC 203 on which the packet was received.
>
> Anyone or a combination of the attributes can be utilized to determine if the packet matches with any user specified rules. Subsequently, if a user specified rule matches with the communication establishing packet, the matched rule is applied to the packet (step 323). If no user specified rule matches the packet, a transparency is applied (step 325).
>
> The user specified rules 209 include user specified static filter rules and user specified dynamic filter rules.
>
> Each entry in the user specified static filter rules includes the attributes discussed above and a value indicating the type of filter to apply to the packet. The types of filters include "permit" filter to forward the packet to its destination, "deny" to discard the packet, "absorb" to apply an application level filter and "a filter all rule" discussed above. In order to provide a finer granularity in the packet filtering, the packet filter of the present invention is extended to include additional fields such as:
>
> (1) TCP flags (SYN, SYN-ACK, URG/PUSH) are provided to block new TCP connections from a certain host, but continue to allow packets of existing connections by adding a filter rule to deny SYN packets from the host; and
>
> (2) Unlike the conventional packet filter rules which only allow a single port to be specified in a rule, the present invention is also configured to allow/deny connections to a particular interface port range. For example, connections to X terminal ports can be denied by specifying a filter rule with the range of X terminal ports specified. (Col. 10, line 51 – Col. 11, line 32).

As can be seen, the relied-upon portions of *Taylor* make no mention whatsoever of specifying an ENABLED field value or a SEVERITY level field value during generation of its configuration file. No such field values are described as included in the configuration file. Further, no other portion of *Taylor* provides such teaching.

In view of the above, *Taylor* fails to teach all elements of claim 8, and therefore claim 8 is not anticipated by *Taylor*. Therefore, the rejection of claim 8 should be withdrawn.

Independent Claim 13

Claim 13 recites in part "compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field." *Taylor* fails to teach at least this element of claim 13.

Taylor does not teach compiling input into a machine-readable signature file that comprises a network-exploit rule and at least one of an ENABLED field and a SEVERITY field. Rather, *Taylor* appears to describe a configuration file that specifies to a firewall rules regarding whether a connection is permitted on particular ports, as well as rules regarding filtering packets for a permitted connection. *See* Col. 5, line 66 – Col. 6, line 60 of *Taylor*. *Taylor* provides no teaching whatsoever of such an ENABLED field or SEVERITY field in its configuration file, as discussed above with claim 8.

In view of the above, *Taylor* fails to teach all elements of claim 13, and therefore claim 13 is not anticipated by *Taylor*. Therefore, the rejection of claim 13 should be withdrawn.

Dependent Claims

Each of dependent claims 2, 14, and 16 depend either directly or indirectly from one of independent claims 1 and 13, and thus inherit all limitations of the respective independent claim from which they depend. It is respectfully submitted that dependent claims 2, 14, and 16 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

IV. Rejections Under 35 U.S.C. § 103 over *Taylor* in view of *Freund*

Claims 3-7, 9-12, 15, and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Taylor* in view of *Freund.* Each of dependent claims 3-7, 9-12, 15, and 17 depend either directly or indirectly from one of independent claims 1, 8, and 13, and thus inherit all limitations of the respective independent claim from which they depend. As discussed above, *Taylor* fails to teach all elements of independent claims 1, 8, and 13. Further, *Freund* is not relied upon as teaching or suggesting the above-identified elements lacking from *Taylor*, nor does it do so. Thus, it is respectfully submitted that dependent claims 3-7, 9-12, 15, and 17 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

V. New Claims

New claims 18-20 each depend either directly or indirectly from one of independent claims 1 and 8, and thus inherit all of the limitations of the respective independent claim from which they depend. Applicant respectfully submits that these claims are allowable over the art of record at least for the reasons discussed above for independent claims 1 and 8.

VI. Conclusion

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response beyond the extension fee dealt with in the accompanying Request for Extension of Time and the associated Fee Transmittal. However, if an additional fee is due, please charge Deposit Account No. 08-2025, under Order No. 10017334-1 from which the undersigned is authorized to draw.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568241989US in an envelope addressed to: M/S Amendment Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: August 7, 2006

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

By:
Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: August 7, 2006
Telephone No. (214) 855-8007